The 2-adic valuation of the cardinality of Jacobians of genus 2 curves over quadratic towers of finite fields *

Ricard Garra, Josep M. Miret, Jordi Pujolàs, Nicolas Thériault

Dep. Matemàtica, Universitat de Lleida, Spain
Dep. Matemáticas, Universidad Santiago de Chile, Chile
{garra,miret, jpujolas}@matematica.udl.cat
nicolas.theriault@usach.cl

June 29, 2018

Abstract

Given a genus 2 curve C defined over a finite field $\mathbb{F}_q$ of odd characteristic such that $2|\#\mathrm{Jac(C)}(\mathbb{F}_q)$, we study the growth of the 2-adic valuation of the cardinality of the Jacobian over a tower of quadratic extensions of $\mathbb{F}_q$. In the cases of simpler regularity, we determine the exponents of the 2-Sylow subgroup of $\mathrm{Jac(C)}(\mathbb{F}_{q^{2^k}})$.

1 Introduction

We consider Jacobians of genus 2 curves C over a finite field $\mathbb{F}_q$ of odd characteristic p with a hyperelliptic model

$$\mathrm{C} : y^2 = f(x), \tag{1}$$

where $f(x) \in \mathbb{F}_q[x]$ has degree 5 or 6 and no multiple roots. We assume our sextic models to have no roots in $\mathbb{F}_q$ because models of degree 6 with a root in $\mathbb{F}_q$ are equivalent to degree 5 models.

We are interested in the powers of 2 in the cardinalities $\#\mathrm{Jac(C)}(\mathbb{F}_{q^{2^k}})$ of the Jacobian as k increases. In principle, the minimal degree d such that $2 \mid \#\mathrm{Jac(C)}(\mathbb{F}_{q^d})$ is either 5 when $f(x)$ is an irreducible quintic, or 3 if $f(x)$ is an irreducible sextic or a product of two irreducible cubics. However, we make the assumption that already over $\mathbb{F}_q$ we have $2 \mid \#\mathrm{Jac(C)}(\mathbb{F}_q)$ because

*Research of the authors was supported in part by grants MTM2013-46949-P (Spanish Ministerio de Ciencia e Innovación), 2014SGR-1666 (Generalitat de Catalunya) and FONDECYT 1151326 (Chile).

we are interested in the cardinality after quadratic extensions. Moreover, our 2-torsion subgroup $\mathrm{Jac(C)}(\mathbb{F}_q)[2]$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^r$ for some $r = 1, \ldots, 4$ because we assume $p \neq 2$. Similarly, we denote the rank of $\mathrm{Jac(C)}(\mathbb{F}_{q^{2^k}})[2]$ by r_k.

Recall that the affine support of (reduced) divisors of order 2 consists of Weierstrass points which are either $\mathbb{F}_q$-rational, or pairs of conjugates of points in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Since the x-coordinates of Weierstrass points are roots of $f(x)$, the 2-rank of the curve can therefore be deduced from the factorization type of the $f(x)$, and we have:

Fact. type $f(x)$	r_0	r_1	$r_k, \forall k \geq 2$
[2,3]	1	2	2
[1,4] [2,4]	1	2	4
[1,1,3]	2	2	2
[1,2,2] [2,2,2]	2	4	4
[1,1,1,2]	3	4	4
[1,1,1,1,1]	4	4	4

Table 1: r_k vs. factorization types of $f(x)$.

Notice cubic irreducible factors in $f(x)$ imply $r_k = 2$ for $k \geq 1$.

Definition 1. *We say $f(x) \in \mathbb{F}_q[x]$ is of inert type if $f(x)$ is a multiple of a cubic irreducible polynomial over $\mathbb{F}_q$, and of split type if it is not.*

In this way, inert factorization types are either [2,3] or [1,1,3], and split factorization types are [1,4], [1,2,2], [1,1,1,2], [1,1,1,1,1], [2,4] or [2,2,2]. Our proofs are slightly different for inert or split types.

We set the notation

$$N_k = \#\mathrm{Jac(C)}(\mathbb{F}_{q^{2^k}}).$$

Our first purpose is to determine the difference of 2-adic valuations

$$v_2(N_{k+1}) - v_2(N_k), \quad k \geq 0.$$

We start by relating the factorization types of $f(x)$ with the coefficients of the characteristic polynomial of the Frobenius endomorphism of $\mathrm{Jac(C)}(\mathbb{F}_q)$. In Proposition 1 of Section 2 we show this difference is strictly positive for every $k \geq 0$, and that it stabilizes to 2 or 4 if $k \geq 4$. These results agree with Iwasawa Theory [8, Theorem 13.13 and p. 130], which for large enough k predicts $v_2(N_k) = \lambda k + \nu$ for $0 \leq \lambda \leq 4$ and ν a constant.

In some of these regular cases, we show how the gain in valuation spreads out in the exponents of the 2-Sylow subgroup $\mathrm{Jac(C)}(\mathbb{F}_{q^{2^k}})[2^\infty]$. Namely, given

$$\mathrm{Jac(C)}(\mathbb{F}_{q^{2^k}})[2^\infty] \cong \mathbb{Z}/2^{n_1^k}\mathbb{Z} \times \mathbb{Z}/2^{n_2^k}\mathbb{Z} \times \mathbb{Z}/2^{n_3^k}\mathbb{Z} \times \mathbb{Z}/2^{n_4^k}\mathbb{Z},$$

with $n_1^k \geq n_2^k \geq n_3^k \geq n_4^k \geq 0$, we obtain the values of n_i^{k+1} for $i = 1, \ldots, 4$ (see Proposition 3 in Section 3).

However, from a computational prespective it is interesting to know how the difference grows also before such a regularity occurs. We devote a large portion of this paper to the case of low exponents $k = 1, 2, 3$ (see Section 4).

A comment on our methodology is due. We study the 2-power torsion in $\mathrm{Jac(C)}(\mathbb{F}_{q^{2^k}})$ from two different points of view. In Section 2 we use the information provided by the 2-valuation of some coefficients of the characteristic polynomial of Frobenius of Jac(C). On the other hand, sections 3 and 4 require the manipulation of Mumford coordinates of divisors, and lean on a characterization of a divisor being in the image of the multiplication-by-2 map.

To do this, we identify Jac(C) with the divisor class group $Pic^0(\mathrm{C})$, and we work with Mumford coordinates $[u(x), v(x)]$ of divisors. Recall that $u(x)$ is a monic polynomial such that $u(x) \mid f(x) - v^2(x)$ and, in genus 2 we have $\deg(u(x)) \leq 2$. In [4], a criterion for a divisor D to be of the form $D = 2D'$ was given in terms of the Mumford coordinates, and computing the pre-images D' explicitly consists in finding the roots of a polynomial $p_D(x) \in \mathbb{F}_q[x]$ of degree 16 attached to $D \in \mathrm{Jac(C)}(\mathbb{F}_q)$ that depends on the the degree of $f(x)$ and on the coefficients (and the degree) of $u(x), v(x)$ (see [3, 5]). We state this in the form of a Lemma.

Lemma 1. *For any $D \in \mathrm{Jac(C)}(\mathbb{F}_{q^{2^k}})$, there exists a polynomial $p_D(x)$ such that $\{D' \in \mathrm{Jac(C)}(\mathbb{F}_{q^{2^k}}) \mid 2D' = D\}$ is obtained from the roots of $p_D(x)$ in $\mathbb{F}_{q^{2^k}}$.*

Proof. $p_D(x)$ is given in [3] if $\deg(f(x)) = 5$ and [5] if $\deg(f(x)) = 6$. □

We use use $p_D(x)$ in the proof of Proposition 3 in Section 3. In Section 4 we use the characterization provided in [4].

2 Information in the characteristic polynomial of Frobenius

Let ϕ_k be the Frobenius endomorphism of $\mathrm{Jac(C)}(\mathbb{F}_{q^{2^k}})$ and let

$$\chi_k(x) = x^4 - a_k x^3 + b_k x^2 - q^{2^k} a_k x + q^{2^{k+1}} \tag{2}$$

be the characteristic polynomial of ϕ_k. It is well known that the coefficients of $\chi_k(x)$ satisfy the bounds $|a_k| \leq 4q^{2^{k-1}}$ and $|b_k| \leq 6q^{2^k}$. More precisely, by [6, Lemma 3.1] we have

$$2|a_k|q^{2^{k-1}} - 2q^{2^k} \leq b_k \leq \frac{a_k^2}{4} + 2q^{2^k}.$$

On the other hand, since

$$N_k = \chi_k(1) = (q^{2^{k+1}} + 1) - a_k(q^{2^k} + 1) + b_k, \tag{3}$$

the assumption $2 \mid \#\mathrm{Jac(C)}(\mathbb{F}_{q^{2^k}})$ clearly implies

$$v_2(b_k) \geq 1 \quad \text{or} \quad b_k = 0. \tag{4}$$

Moreover, the coefficients a_k, b_k satisfy the recurrences (see [2])

$$a_{k+1} = a_k^2 - 2b_k, \quad b_{k+1} = b_k^2 - 2q^{2^k} a_k^2 + 2q^{2^{k+1}}. \tag{5}$$

From these, we immediately have

$$N_{k+1} = N_k\Big((q^{2^{k+1}} + 1) + a_k(q^{2^k} + 1) + b_k\Big), \quad \forall k \geq 0. \tag{6}$$

Hence we have identified the 2-adic valuations responsible for the next cardinality N_{k+1}, namely

$$\nu_k = v_2(N_k), \quad \overline{\nu_k} = v_2((q^{2^{k+1}} + 1) + a_k(q^{2^k} + 1) + b_k).$$

Indeed, from (6) immediately

$$\nu_{k+1} = \nu_k + \overline{\nu_k}. \tag{7}$$

Moreover, by substituting a_k and b_k from (5) in (6), we obtain:

$$N_{k+1} = N_k\Big((a_{k-1}(q^{2^{k-1}} - 1))^2 + (q^{2^k} + 1 - b_{k-1})^2\Big), \quad \forall k \geq 1. \tag{8}$$

Lemma 2. *Let* $\chi_k(x) = x^4 - a_k x^3 + b_k x^2 - q^{2^k} a_k x + q^{2^{k+1}}$ *be the characteristic polynomial of the Frobenius endomorphism of* $\mathrm{Jac(C)}(\mathbb{F}_{q^{2^k}})$.

i) If $\nu_k \neq v_2(a_k(q^{2^k} + 1)) + 1$, *then* $\overline{\nu_k} = \min\{\nu_k, v_2(a_k(q^{2^k} + 1)) + 1\}$.

ii) If $\nu_k = v_2(a_k(q^{2^k} + 1)) + 1$, *then* $\overline{\nu_k} \geq \nu_k + 1$.

Proof. Clearly

$$(q^{2^{k+1}} + 1) + a_k(q^{2^k} + 1) + b_k = \Big((q^{2^{k+1}} + 1) - a_k(q^{2^k} + 1) + b_k\Big) + 2 \cdot a_k(q^{2^k} + 1).$$

Hence

$$\overline{\nu_k} = \min\{\nu_k, v_2(a_k(q^{2^k} + 1)) + 1\}$$

if $\nu_k \neq v_2(a_k(q^{2^k} + 1)) + 1$. Otherwise, $\overline{\nu_k} \geq \nu_k + 1$. □

From (7) and Lemma 2 we immediately obtain the strict growth.

Corollary 1. *The 2-adic valuation above satisfies*

$$\nu_k < \nu_{k+1}, \quad \forall k \geq 0.$$

We now identify the coefficients of Frobenius involved in our increment.

Proposition 1. *Let* C *be a curve and let* $\chi_k(x)$ *be the characteristic polynomial of Frobenius of* $\mathrm{Jac(C)}(\mathbb{F}_{q^{2^k}})$.

i) If $v_2(a_0) = 0$, *then*

$$\nu_{k+1} = \nu_k + 2, \quad \forall k \geq 2,$$

ii) If $v_2(a_0) \geq 1$ *or* $a_0 = 0$, *then*

$$\nu_{k+1} = \nu_k + 4, \quad \forall k \geq 3,$$

Proof. If $v_2(a_0) = 0$, then $v_2(a_1) = v_2(a_0^2 - 2b_0) = 0$. By (5), $v_2(a_k) = 0, \forall k \geq 2$. Since $v_2(q^{2^k} + 1) = 1, \forall k \geq 1$, we know that $v_2(a_k(q^{2^k} + 1)) + 1 = 2, \forall k \geq 1$. Therefore $\nu_{k+1} \geq \nu_k + \min\{\nu_k, 2\}$ by Lemma 2. But also $\nu_k > 2, \forall k \geq 2$ by Corollary 1, so we can assure $\nu_{k+1} = \nu_k + 2, \forall k \geq 2$.

If $v_2(a_0) \geq 1$ or $a_0 = 0$, since also $v_2(b_0) \geq 1$ or $b_0 = 0$ by (4), we obtain $v_2(a_1) \geq 2, v_2(b_1) = 1$ and $v_2(a_1(q^2 + 1)) + 1 \geq 4$ from (5). Since $v_2(b_k) = 1, \forall k \geq 1$, then $v_2(a_k) = 2$ and $v_2(a_k(q^{2^k} + 1)) + 1 = 4, \forall k \geq 2$. By Corollary 1, $\nu_k > 4, \forall k \geq 3$, so by Lemma 2 we can assure $\nu_{k+1} = \nu_k + 4, \forall k \geq 3$. □

Remark 1. *If* $v_2(a_0) \geq 1$ *and* $\nu_0 \geq 2$, *then* $\nu_{k+1} = \nu_k + 4$, $\forall k \geq 2$.

For exponents $k \leq 3$ we need a bit more. Indeed, for $k \geq 1$ (8) implies

$$\overline{\nu_k} = v_2\Big((a_{k-1}(q^{2^{k-1}} - 1))^2 + (q^{2^k} + 1 - b_{k-1})^2\Big), \quad \forall k \geq 1. \tag{9}$$

We now restate (9) in form of an equivalent Lemma. Let

$$A_k = v_2(a_{k-1}(q^{2^{k-1}} - 1)) \text{ and } B_k = v_2(q^{2^k} + 1 - b_{k-1}). \tag{10}$$

Lemma 3. *Let* A_k, B_k, *as above. For* $k \geq 1$, *we have*

i) If $A_k \neq B_k$, *then* $\overline{\nu_k} = 2\min\{A_k, B_k\}$.

ii) If $A_k = B_k$, *then* $\overline{\nu_k} = 2A_k + 1$.

We now define

$$t_k = v_2(q^{2^{k-1}} - 1).$$

Note that $t_2 \geq 3$ and $t_k \geq k + 1$ for $k \geq 2$.

Corollary 2. *Let A_k, B_k as above. For $k \geq 2$,*

$$A_k = t_k + v_2(a_{k-2}^2 - 2b_{k-2}),$$
$$B_k = v_2((q^{2^{k-1}} - 1)^2 + b_{k-2}^2 + 2a_{k-2}^2 q^{2^{k-2}}).$$

Moreover, $\overline{\nu}_k \leq 4t_k + 3$, and $\overline{\nu}_k$ is even unless $v_2(b_{k-2}) = v_2(a_{k-2}) = t_k$.

Proof. The expressions in a_{k-2} and b_{k-2} follow from the recurrences (5). Note that $A_k = v_2(a_{k-1}(q^{2^{k-1}} - 1)) = t_k + v_2(a_{k-1})$. Hence, if $v_2(b_{k-2}) \neq t_k$, then

$$B_k = \min\{2t_k, 2v_2(b_{k-2}), 2v_2(a_{k-2}) + 1\} \tag{11}$$

since the first two terms in $(q^{2^{k-1}} - 1)^2 - b_{k-2}^2 + 2qa_{k-2}^2$ have distinct even valuations and the third term has odd valuation. Otherwise $v_2(b_{k-2}) = t_k$ implies $v_2((q^{2^{k-1}} - 1)^2 - b_{k-2}^2) \geq 2t_k + 3$. The remaining claims follow from the following possibilities.

- Assume $v_2(b_{k-2}) \neq t_k$.
  - If $v_2(a_{k-1}) < v_2(b_{k-2}) + 1$ then $2v_2(a_{k-2}) = v_2(a_{k-1})$. Therefore from (11) we obtain $B_k \leq 2v_2(a_{k-2}) + 1$ and we have $A_k = t_k + 2v_2(a_{k-2})$. Hence $B_k < A_k$ and $\overline{\nu_k} = 2B_k \leq 4t_k$.
  - If $v_2(a_{k-1}) > v_2(b_{k-2}) + 1$, then $2v_2(a_{k-2}) = v_2(b_{k-2}) + 1$. Hence we can take $B_k \leq v_2(b_{k-2}) + 2$ and we have $A_k > t_k + v_2(b_{k-2}) + 1$. We then obtain $B_k < A_k$ and $\overline{\nu_k} = 2B_k \leq 4t_k$.
  - Otherwise $v_2(a_{k-1}) = v_2(b_{k-2}) + 1$. If $v_2(b_{k-2}) < t_k$, then $A_k = t_k + v_2(b_{k-2}) + 1$ and $B_k \leq 2v_2(b_{k-2}) < t_k + v_2(b_{k-2})$, so $B_k < A_K$. Otherwise, $v_2(b_{k-2}) > t_k$ yields $A_k = t_k + v_2(b_{k-2}) + 1$ and $B_k \leq 2t_k < t_k + v_2(b_{k-2})$, so $B_k < A_k$. Hence $\overline{\nu_k} = 2B_k \leq 4t_k$.
- Otherwise, let $v_2(b_{k-2}) = t_k$.
  - If $v_2(a_{k-2}) < t_k$ then $v_2(2q^{2^{k-2}} a_{k-2}^2) < 2t_k - 1$, so $B_k = 2v_2(a_{k-2}) + 1$. On the other hand, either $v_2(a_{k-1}) = \min\{2v_2(a_{k-2}), t_k + 1\}$ or $v_2(a_{k-1}) \geq t_k + 2$, so $A_k = t_k + 2v_2(a_{k-1})$ or $A_k \geq 2t_k + 1$ (only if $v_2(a_{k-1}) > t_k/2$). Since $t_k \geq 3$, then $A_k > B_k$ and we have $\overline{\nu_k} = 2B_k \leq 4t_k$.
  - If $v_2(a_{k-2}) > t_k$, then $A_k = 2t_k + 1$, and we have $v_2(2q^{2^{k-2}} a_{k-2}^2) \geq 2t_k + 3$, hence $B_k \geq 2t_k + 3 > A_k$. Hence $\overline{\nu_k} = 2A_k = 4t_k + 2$.
  - Finally, let $v_2(a_{k-2}) = t_k$. Then $A_k = 2t_k + 1$, and $v_2(2q^{2^{k-2}} a_{k-2}^2) = 2t_k + 1 = B_k$. Since $B_k = A_k$, we have $\overline{\nu_k} = 4t_k + 3$.

□

3 General results on increment and exponents

We say a divisor $D \in \mathrm{Jac(C)}(\mathbb{F}_{q^{2^k}})$ has a bisection if there exists $D' \in \mathrm{Jac(C)}(\mathbb{F}_{q^{2^k}})$ such that $2D' = D$. Our first result in this Section describes the situation for which every divisor has a bisection "a quadratic extension away".

Proposition 2. *Let* C *be a curve such that* $r_{k+1} = r_k$. *If* $D \in \mathrm{Jac(C)}(\mathbb{F}_{q^{2^k}})$ *has no bisections, then* D *has at least one bisection over* $\mathbb{F}_{q^{2^{k+1}}}$.

Proof. Consider the case $r_k = 4$. Let θ_i be the roots of $f(x)$ and $D = [u(x), v(x)] \in \mathrm{Jac(C)}(\mathbb{F}_{q^{2^k}})$. From [4] we know D has a bisection if and only if $u(\theta_i)$ is a square in $\mathbb{F}_{q^{2^k}}$, $\forall i$. But all the $u(\theta_i)$ are squares in $\mathbb{F}_{q^{2^{k+1}}}$. Thus D has a bisection over $\mathbb{F}_{q^{2^{k+1}}}$. When $r_k = 2$, the claim follows similarly. □

In our next proposition we use the polynomial $p_D(x)$ introduced in Lemma 1.

Proposition 3. *Let* C *be a genus 2 curve over* $\mathbb{F}_{q^{2^k}}$ *whose Jacobian has a non-trivial 2-Sylow subgroup isomorphic to* $\mathbb{Z}/2^{n_1^k}\mathbb{Z} \times \mathbb{Z}/2^{n_2^k}\mathbb{Z} \times \mathbb{Z}/2^{n_3^k}\mathbb{Z} \times \mathbb{Z}/2^{n_4^k}\mathbb{Z}$, *with* $n_1^k \geq n_2^k \geq n_3^k \geq n_4^k \geq 0$.

i) If the type of $f(x)$ *is inert, then* $\nu_{k+1} = \nu_k + 2$ *and*

$$(n_1^{k+1}, n_2^{k+1}) = (n_1^k + 1, n_2^k + 1), \quad \forall k \geq 2.$$

ii) If the type of $f(x)$ *is split, then* $\nu_{k+1} = \nu_k + 4$ *and*

$$(n_1^{k+1}, n_2^{k+1}, n_3^{k+1}, n_4^{k+1}) = (n_1^k + 1, n_2^k + 1, n_3^k + 1, n_4^k + 1), \quad \forall k \geq 3.$$

Proof. By Proposition 2, all $D \in \mathrm{Jac(C)}(\mathbb{F}_{q^{2^k}})[2^\infty]$ have a bisection over $\mathbb{F}_{q^{2^k}}$ when $r_k = 4$, and by Proposition 1 we know that, after a certain number of quadratic extensions, the valuation ν_{k+1} increases by 2 or 4, depending on the value of a_0.

If the type of $f(x)$ is split, then the rank of $\mathrm{Jac(C)}(\mathbb{F}_q)[2]$ is 4 after at most 2 quadratic extensions. As a consequence, the exponents of $\mathrm{Jac(C)}(\mathbb{F}_{q^{2^k}})[2^\infty]$, with $k \geq 2$, must be $(n_1^k, n_2^k, n_3^k, n_4^k)$, $n_4^k > 0$. Since every divisor has a bisection over $\mathbb{F}_{q^{2^{k+1}}}$, the only option is that $\nu_{k+1} = \nu_k + 4$ for $k \geq 3$. Therefore each exponent increases exactly by 1, proving *ii)*.

If the type of $f(x)$ is inert, then the rank of $\mathrm{Jac(C)}(\mathbb{F}_q)[2]$ after one quadratic extension is 2, and the exponents of $\mathrm{Jac(C)}(\mathbb{F}_{q^{2^k}})[2^\infty]$ are (n_1^k, n_2^k). Over a cubic extension, the rank of $\mathrm{Jac(C)}(\mathbb{F}_{q^{2^k \cdot 3}})[2]$ becomes 4. From [3, Theorem 2], we know that the only possible factorization of the polynomial $p_D(x)$ for a divisor D which does not have bisection is [2,2,6,6]. The factorization of $p_D(x)$ over this cubic extension becomes $[2, \ldots, 2]$. Therefore $\mathrm{Jac(C)}(\mathbb{F}_{q^{2^k \cdot 3}})[2^\infty]$ has exponents $(n_1^k, n_2^k, n_3^k, n_4^k)$, with $n_4^k > 0$.

Over a second quadratic extension, the exponents of the new 2-Sylow subgroup $\mathrm{Jac(C)}(\mathbb{F}_{q^{3\cdot 2^{k+1}}})[2^\infty]$ must be $(n_1^k+1, n_2^k+1, n_3^k+1, n_4^k+1)$, because by *ii)* each level increases exactly by 1. Hence, our 2-Sylow subgroup $\mathrm{Jac(C)}(\mathbb{F}_{q^{2^{k+1}}})[2^\infty]$ must have exponents (n_1^k+1, n_2^k+1), and therefore $\nu_{k+1} = \nu_k + 2$, proving *i)*. □

Corollary 3. *Let* C *be a curve with* $\chi_k(x)$ *as in (2).*

i) If the type of $f(x)$ *is inert, then* $v_2(a_0) = 0$.

ii) If the type of $f(x)$ *is split, then either* $v_2(a_0) \geq 1$ *or* $a_0 = 0$.

Proof. Immediate from Proposition 3 and Corollary 1. □

In Table 2 below we collect the information about the 2-adic valuation of a_0 and b_0 we deduce from ν_0 in (3) and the factorization type of $f(x)$.

$f(x)$ **type**	ν_0	$a_0 \pmod 2$	$b_0 \pmod 4$
inert , $q \equiv 1 \pmod 4$	1	1	2
inert , $q \equiv 3 \pmod 4$	1	1	0
inert, $q \equiv 1 \pmod 4$	≥ 2	1	0
inert, $q \equiv 3 \pmod 4$	≥ 2	1	2
split	1	0	0
split	≥ 2	0	2

Table 2: 2-adic data on a_0 and b_0

The information in Table 2 might be useful in the initial steps of the genus 2 versions of the SEA algorithm for point counting [1].

4 The case of low exponents $k = 1, 2, 3$

With the previous results, we now study the increment of the 2-adic valuation ν_k for $k = 1, 2, 3$ in terms of q, ν_0 and the 2-adic valuation of a_0. We treat split and inert types separately.

Inert types

Inert types satisfy $v_2(a_0) = 0$ by Corollary 3, hence $v_2(a_k) = 0 \, \forall k$ by (5). Therefore the valuation $v_2(a_0(q+1))$ is exactly 1 if $q \equiv 1 \pmod 4$, and ≥ 2 if $q \equiv 3 \pmod 4$, while $v_2(a_k(q^{2^k}+1)) = 1, \forall k \geq 1$.

With this and Lemma 2 the values of ν_1 and ν_2 follow. These are shown in Tables 3 and 4 below, where only two entries need further justification.

$f(x)$ **inert**	ν_0	ν_1	ν_2
$r_0 = 1$	1	2	$^{(1)}[6, 2t_1 + 3]$
$r_0 = 1, 2$	2	≥ 5	$\nu_1 + 2$
	≥ 3	$\nu_0 + 2$	$\nu_1 + 2$

Table 3: Valuations ν_1, ν_2 when $a_0 \neq 0$, $v_2(a_0) = 0$ and $q \equiv 1 \pmod 4$.

$f(x)$ **inert**	ν_0	ν_1	ν_2
$r_0 = 1$	1	2	$^{(2)}5$
$r_0 = 1, 2$	2	4	6
	$[3, t_2 - 1]$	$2\nu_0$	$\nu_1 + 2$
	t_2	$\geq 2\nu_0 + 1$	$\nu_1 + 2$
	$\geq t_2 + 1$	$\nu_0 + t_2$	$\nu_1 + 2$

Table 4: Valuations ν_1, ν_2 when $a_0 \neq 0$, $v_2(a_0) = 0$ and $q \equiv 3 \pmod 4$.

(1) Here $A_1 = v_2(a_0(q-1)) = t_1 \geq 2$. Since $\nu_0 = v_2((q^2+1) - a_0(q+1) + b_0) = 1$, then $v_2(b_0) \geq 2$, and then $B_1 \geq 2$. By Lemma 3 we have $4 \leq \overline{\nu_1} \leq 2A_1 + 1 = 2t_1 + 1$ (which is even unless the upper bound is reached, when $B_1 = t_1$).

(2) Here $A_1 = 1$. Since $\nu_0 = v_2((q^2+1) - a_0(q+1) + b_0) = 1$, it turns out that $v_2(b_0) \geq 2$, so $B_1 = v_2(q^2+1-b_0) = 1$. Hence $\nu_2 = \nu_1 + 2A_1 + 1 = 5$ by Lemma 3.

Example 1. Consider the curves

$$\begin{aligned} \mathrm{C}_1 : y^2 &= x^5 + 42x^3 + 127x^2 + 82x + 18, \\ \mathrm{C}_2 : y^2 &= x^5 + 51x^3 + 4x^2 + 78x + 26, \end{aligned}$$

both defined over $\mathbb{F}_q$ with $q = 131 \equiv 3 \pmod 4$ and $t_2 = 3$. Their factorization types are [1,1,3], so the 1st rank is $r_0 = 2$. The values of ν_1, ν_2 are:

	$f(x)$	ν_0	ν_1	ν_2
C_1	[1,1,3]	3	7	9
C_2	[1,1,3]	3	17	19

Split types

Split types satisfy $v_2(a_0) \geq 1$ or $a_0 = 0$ by Corollary 3. Therefore, if $a_0 \neq 0$ the valuation $v_2(a_0(q+1))$ is ≥ 2 if $q \equiv 1 \pmod 4$ and ≥ 3 if $q \equiv 3 \pmod 4$, while $a_0 = 0$ implies $\nu_1 = 2 \cdot \nu_0$ because then $N_1 = N_0^2$. In any case $v_2(b_k) = 1, \forall k \geq 1$ by (5). Introducing ν_0 we deduce more rules.

- By (3), $\nu_0 > 1$ if and only if $v_2(b_0) = 1$.
  - If $a_0 = 0$ or $v_2(a_0) > 1$, then $v_2(a_1) = 2$ and $v_2(a_1(q^2+1)) = 3$.
  - If $v_2(a_0) = 1$, then $v_2(a_1) \geq 3$, and therefore $v_2(a_1(q^2+1)) \geq 4$.
- By (3), $\nu_0 = 1$ if and only if $v_2(b_0) \geq 2$ or $b_0 = 0$, which also implies $r_0 = 1$. Therefore, independently of the value of a_0, $v_2(a_1) \geq 2$ by (5).

Since in all cases $v_2(a_1) \geq 2$, we obtain $v_2(a_2) = 2$ by (5).

Now ν_1, ν_2, ν_3 follow by Lemma 2. These are shown in Tables 5 and 6.

$f(x)$ **split**	ν_0	ν_1	ν_2	ν_3
$r_0 = 1$	1	2	4	$^{(1)}[10, 4t_2+7]$
$r_0 = 1, 2$	2	4	$^{(2)} \geq 8$	$\nu_2 + 4$
$r_0 = 1, 2, 3$	≥ 3	$^{(3)} \geq \nu_0 + s$	$^{(4)}[\nu_1+4, \nu_1+2t_1+3]$	$\nu_2 + 4$
$r_0 = 4$	≥ 4	$\geq \nu_0 + 4$	$\nu_1 + 4$	$\nu_2 + 4$

Table 5: Valuations ν_1, ν_2, ν_3 when $a_0 \neq 0, \quad v_2(a_0) \geq 1$.

$f(x)$ **split**	ν_0	ν_1	ν_2	ν_3
$r_0 = 1$	1	2	4	$^{(5)}[12, 4t_2+6]$
$r_0 = 1, 2$	2	4	$^{(6)} \geq 10$	$\nu_2 + 4$
$r_0 = 1, 2, 3, 4$	≥ 3	$2 \cdot \nu_0$	$\nu_1 + 4$	$\nu_2 + 4$

Table 6: Valuations ν_1, ν_2, ν_3 when $a_0 = 0$.

(1) Notice $A_2 = v_2(a_1(q^2-1)) \geq 5$. Since $\nu_1 = v_2((q^4+1) - a_1(q^2+1) + b_1) = 2$, we have $v_2(q^4+1+b_1) = 2$. Then $B_2 = v_2(q^4+1-b_1) \geq 3$, hence $\nu_3 \geq 10$ by Lemma 3. By Corollary 2, $\overline{\nu_2} \leq 4t_2+3$ is even unless $v_2(a_0) = v_2(b_0) = t_2$, in which case the upper bound is attained.

(2) Since $\overline{\nu_0} = \nu_0 = 2$, then $v_2(a_0(q+1)) \geq 3$ and $v_2(q^2+1+b_0) = 2$, and we have that $B_1 \geq 3$. On the other hand, $A_1 = t_1 + v_2(a_0) \geq 2$. Then $\overline{\nu}_1 \geq 4$ and $\overline{\nu}_1 \neq 5$ since the case $A_1 = B_1 = 2$ is excluded.

(3) By Lemma 2,

$$s = \begin{cases} 3 & \text{if } q \equiv 1 \pmod 4, \\ 3 & \text{if } q \equiv 3 \pmod 4 \text{ and } \nu_0 = 3 \text{ (in which case } \nu_1 = \nu_0 + s = 6), \\ 4 & \text{otherwise.} \end{cases}$$

(4) We have $v_2(b_0) = 1$, $A_1 = v_2(a_0) + t_1$, $B_1 = v_2(q^2+1-b_0) = v_2(N_0 + a_0(q+1) - 2b_0)$. If $v_2(a_0) > 1$, then $A_1 > 2, B_1 = 2$, and by Lemma 3

the lower bound is $\overline{\nu_1} = 2B_1 = 4$. If $v_2(a_0) = 1$, then $A_1 = t_1 + 1$, so the upper bound is achieved when $A_1 = B_1$. Therefore $\overline{\nu_1} = 2A_1 + 1 = 2t_1 + 3$ and all other values of $\overline{\nu_1}$ are even.

(5) Here we have $A_2 = v_2(a_1) + t_2 = v_2(b_0) + t_2 + 1$ and $B_2 = v_2(q^4 + 1 - b_1) = v_2((q^2-1)^2 - b_0^2)$. Since $v_2(b_0) \geq 2$ then $A_2 \geq 6$ and $B_2 \geq 4$. Therefore $\overline{\nu_2} \geq 8$ by Lemma 3. Hence a lower bound of ν_3 is 12.

From Corollary 2, $\overline{\nu_2} \leq 4t_2 + 3$ is even unless $v_2(a_0) = v_2(b_0) = t_2$. Since $a_0 = 0$, then $v_2(a_0) \neq t_2$, so $\overline{\nu_2} \leq 4t_2 + 2$.

(6) It can be easily seen that $B_1 = v_2(q^2 + 1 - b_0) \geq 3$. Since $a_0 = 0$, then $A_1 \neq B_1$, so $\overline{\nu_1} \geq 6$ and even by Lemma 3.

Example 2. Consider the curves

$$\begin{aligned} \mathrm{C}_3 : y^2 &= x^5 + 136x^3 + 80x^2 + 32x + 61, \\ \mathrm{C}_4 : y^2 &= x^5 + 53x^3 + 83x^2 + 6x + 67, \\ \mathrm{C}_5 : y^2 &= x^5 + 9x^3 + 86x^2 + 136x + 56, \end{aligned}$$

defined over $\mathbb{F}_q$ with $q = 137 \equiv 1 \pmod 4$, $t_1 = 3$ and $t_2 = 4$. Their factorization types are [1,4], so $r_0 = 1$. The values of ν_k and a_0 are:

	$f(x)$	a_0	ν_0	ν_1	ν_2	ν_3
C_3	[1,4]	0	1	2	4	12
C_4	[1,4]	0	1	2	4	16
C_5	[1,4]	$\neq 0$	5	8	14	18

Example 3. Consider the curves

$$\begin{aligned} \mathrm{C}_6 : y^2 &= x^5 + 36x^3 + 49x^2 + 72x + 7, \\ \mathrm{C}_7 : y^2 &= x^5 + 78x^3 + 110x^2 + 93x + 17, \end{aligned}$$

both defined over $\mathbb{F}_q$ with $q = 131 \equiv 3 \pmod 4$ and $t_1 = 1$. Their factorization type is [1,1,1,2], so $r_0 = 3$, and $a_0 \neq 0$. The values of ν_k are:

	$f(x)$	ν_0	ν_1	ν_2	ν_3
C_6	[1,1,1,2]	4	8	12	16
C_7	[1,1,1,2]	4	9	14	18

4.1 Variation of some 2-Sylow exponents for $k = 1, 2, 3$

We now study the exponents of the 2-Sylow subgroup of $\mathrm{Jac(C)}(\mathbb{F}_{q^{2^k}})[2^\infty]$ when $k \leq 3$ in some cases. We are going to use the ideas in [4], which give a characterisation for a divisor $D = [u(x), v(x)] \in \mathrm{Jac(C)}(\mathbb{F}_q)$ to have bisections in $\mathrm{Jac(C)}(\mathbb{F}_q)$ in terms of $\prod_{i=1}^{d} u(\theta_i)$ being a square for all irreducible factors $h(x) = \prod_{i=1}^{d}(x - \theta_i)$ of $f(x)$.

Lemma 4. *Let $f(x)$ be an inert type [2,3] over $\mathbb{F}_q$ whose quadratic irreducible factor $g(x)$ splits as $g(x) = (x-b)(x-b^q)$ in $\mathbb{F}_{q^2}[x]$ and whose cubic splits as $h(x) = \prod_{i=1}^{3}(x-\theta_i)$ in $\mathbb{F}_{q^3}[x]$. Then*

i) The divisor $[g(x), 0]$ has bisections in $\mathrm{Jac(C)}(\mathbb{F}_q)$ if and only if both $h(b)h(b^q)$ and $\prod_{i=1}^{3} g(\theta_i)$ are squares in $\mathbb{F}_q$.

ii) If $q \equiv 1 \pmod 4$ then neither of the divisors $[x-b, 0]$ and $[x-b^q, 0]$ have bisections in $\mathrm{Jac(C)}(\mathbb{F}_{q^2})$.

iii) If $q \equiv 3 \pmod 4$, the divisor $[x-b, 0]$ (resp. $[x-b^q, 0]$) has bisections in $\mathrm{Jac(C)}(\mathbb{F}_{q^2})$ if and only if $h(b)$ (resp. $h(b^q)$) is a square in $\mathbb{F}_{q^2}$.

Proof. Claim i) follows from [4, Theorem 4.7]. Claims ii) and iii) can be derived from [4, Proposition 3.3] taking into account that $b-b^q$ is a quadratic residue in $\mathbb{F}_{q^2}$ if and only if $q \equiv 3 \pmod 4$. □

Lemma 5. *Let $f(x)$ be a split type [1,4] over $\mathbb{F}_q$ with $f(x) = (x-a)s(x)$. Let $s(x) = g(x)g^q(x)$ in $\mathbb{F}_{q^2}[x]$ with $g(x)$ irreducible of degree 2 and $s(x) = \prod_{i=0}^{3}(x-b^{q^i})$ in $\mathbb{F}_{q^4}[x]$.*

i) The divisor $[x-a, 0]$ has bisections in $\mathrm{Jac(C)}(\mathbb{F}_q)$ if and only if $s(a)$ is a square in $\mathbb{F}_q$.

ii) The divisor $[g(x), 0]$ has bisections in $\mathrm{Jac(C)}(\mathbb{F}_{q^2})$ if and only if $g(a)$ is a square in $\mathbb{F}_{q^2}$.

iii) The divisor $[x-b, 0]$ has bisections in $\mathrm{Jac(C)}(\mathbb{F}_{q^4})$ if and only if $b-a$ and $b-b^{q^i}$, $i = 1, 2, 3$ are all squares in $\mathbb{F}_{q^4}$.

Proof. Claim i) can be deduced from [4, Proposition 3.3]. Claim ii) follows from [4, Theorem 4.7] taking into account that $g^q(b)g^q(b^{q^2})$ is square in $\mathbb{F}_{q^2}$. Claim iii) follows from [4, Theorem 3.1] □

Definition 2. *For any divisor $W \in \mathrm{Jac(C)}(\mathbb{F}_{q^{2^k}})$, we define the branch of W as*

$$\mathcal{B}_W^{\infty}(\mathbb{F}_{q^{2^k}}) = \{D \in \mathrm{Jac(C)}(\mathbb{F}_{q^{2^k}}) \mid 2^t D = W \text{ for some } t \in \mathbb{N}\}.$$

For $D \in \mathrm{Jac(C}(\mathbb{F}_{q^{2^k}}))$, we call the smallest natural number r such that $2^r D = 0$ the level of D (that is to say, D has order exactly 2^r). For a given level $r > 0$, and a given divisor W of level s, we let

$$\mathcal{B}_W^{r}(\mathbb{F}_{q^{2^k}}) = \{D \in \mathrm{Jac(C)}(\mathbb{F}_{q^{2^k}}) \mid 2^{r-s} D = W\}.$$

Note that $\mathcal{B}_{\mathcal{O}}^{\infty}(\mathbb{F}_{q^{2^k}}) = \mathrm{Jac(C)}(\mathbb{F}_{q^{2^k}})[2^{\infty}]$ and, by letting the set of non-trivial 2-torsion divisors be $\mathcal{W} = \{[x-b, 0], [x-b^q, 0], [g(x), 0]\}$, it is clear that we have a partition

$$\mathcal{B}_{\mathcal{O}}^{r}(\mathbb{F}_{q^{2^k}}) = \bigcup_{W \in \mathcal{W}} \mathcal{B}_W^{r}(\mathbb{F}_{q^{2^k}}) \cup \{\mathcal{O}\}.$$

Lemma 6. *Let $f(x)$ be an inert type [2,3] over $\mathbb{F}_q$ whose quadratic factor $g(x)$ splits as $g(x) = (x-b)(x-b^q)$ over $\mathbb{F}_{q^2}$. Assume there are no divisors of order 4 in $\mathrm{Jac}(C)(\mathbb{F}_{q^2})$, that $k \geq 2$ and that there is a nonzero divisor $D_b \in \mathcal{B}^{\infty}_{[x-b,0]}(\mathbb{F}_{q^{2^k}})$ of some level $r \geq 1$. Then every divisor $\bar{D} \in \mathcal{B}^{r}_{[g(x),0]}(\mathbb{F}_{q^{2^k}})$ is of the form $\bar{D} = D + D^q$ with $D \in \mathcal{B}^{r}_{[x-b,0]}(\mathbb{F}_{q^{2^k}})$ or $D \in \mathcal{B}^{r}_{[x-b^q,0]}(\mathbb{F}_{q^{2^k}})$.*

Proof. We argue by counting divisors in branches of the 2-Sylow tree. With our assumptions, group theory implies

$$\#\mathcal{B}^{r}_{[x-b,0]}(\mathbb{F}_{q^{2^k}}) = \#\mathcal{B}^{r}_{[x-b^q,0]}(\mathbb{F}_{q^{2^k}}) = \#\mathcal{B}^{r}_{[g(x),0]}(\mathbb{F}_{q^{2^k}}).$$

We first determine in how many ways one can obtain the same divisor with an expression of the form $D + D^q$. For this, consider the endomorphism

$$\begin{array}{ccc} \varphi : \mathrm{Jac(C)}(\mathbb{F}_{q^{2^k}}) & \to & \mathrm{Jac(C)}(\mathbb{F}_{q^{2^k}}) \\ D & \mapsto & D + D^q. \end{array}$$

Since $\mathcal{B}^{r}_{[x-b,0]}(\mathbb{F}_{q^{2^k}})^{\sigma} = \mathcal{B}^{r}_{[x-b^q,0]}(\mathbb{F}_{q^{2^k}})$ and $\mathcal{B}^{r}_{[x-b^q,0]}(\mathbb{F}_{q^{2^k}})^{\sigma} = \mathcal{B}^{r}_{[x-b,0]}(\mathbb{F}_{q^{2^k}})$, we have $\varphi\Big(\mathcal{B}^{r}_{[x-b,0]}(\mathbb{F}_{q^{2^k}}) \cup \mathcal{B}^{r}_{[x-b^q,0]}(\mathbb{F}_{q^{2^k}})\Big) \subset \mathcal{B}^{r}_{[g(x),0]}(\mathbb{F}_{q^{2^k}})$. We now consider two distinct divisors D and D' in $\mathcal{B}^{r}_{\mathcal{O}}(\mathbb{F}_{q^{2^k}})$ such that

$$D + D^q = D' + D'^q.$$

Let $D_1 = D' - D \neq 0$, then $2^r D_1 = 0$ and $D' + D'^q = D + D_1 + D^q + {D_1}^q$, so we must have $D_1 + {D_1}^q = 0$. This implies $D_1^{\sigma} = -D_1$, and we have two cases to consider:

- If D_1 has order 2, then $D_1^{\sigma} = D_1$, i.e. $D_1 \in \mathrm{Jac}(C)(\mathbb{F}_q)$. Due to the group structure, this implies $D_1 = [g(x), 0]$.
- If D_1 has order 4 or higher, then $(D_1^{\sigma})^{\sigma} = D_1$, i.e. $D_1 \in \mathrm{Jac}(C)(\mathbb{F}_{q^2})$. However, there are no divisors of order greater than 2 in $\mathrm{Jac}(C)(\mathbb{F}_{q^2})$, so this case cannot occur.

Hence $ker(\varphi) = \langle [g(x), 0] \rangle$, so for any divisor $\overline{D} \in im(\phi)$ there are two different possibilities to write it as a sum of conjugates:

$$D + D^q \text{ and } \; D + [g(x), 0] + (D + [g(x), 0])^q.$$

Since D and $D + [g(x), 0]$ are in the same branch when $r > 1$, this shows

$$\varphi(\mathcal{B}^{r}_{[x-b,0]}(\mathbb{F}_{q^{2^k}})) \cap \varphi(\mathcal{B}^{r}_{[x-b^q,0]}(\mathbb{F}_{q^{2^k}})) = \emptyset.$$

Furthermore, since the three branches are of the same size and the kernel of φ has order 2, then

$$\varphi\Big(\mathcal{B}^{r}_{[x-b,0]}(\mathbb{F}_{q^{2^k}}) \cup \mathcal{B}^{r}_{[x-b^q,0]}(\mathbb{F}_{q^{2^k}})\Big) = \mathcal{B}^{r}_{[g(x),0]}(\mathbb{F}_{q^{2^k}}).$$

□

Lemma 7. *Let $f(x) = (x-a)s(x)$ be a split type [1,4] over $\mathbb{F}_q$ whose quartic factor splits as $s(x) = g(x)g^q(x)$ over $\mathbb{F}_{q^2}$ and $s(x) = \prod_{i=0}^{3}(x - b^{q^i})$ over $\mathbb{F}_{q^4}$. Assume there are no divisors of order 4 in $\mathrm{Jac}(C)(\mathbb{F}_{q^2})$.*

i) Assume that $k \geq 2$ and that there is a nonzero divisor $D_c \in \mathcal{B}^{\infty}_{[g(x),0]}(\mathbb{F}_{q^{2^k}})$ of some level $r \geq 1$. Then every $\bar{D} \in \mathcal{B}^{r}_{[(x-a),0]}(\mathbb{F}_{q^{2^k}})$ is of the form $\bar{D} = D + D^q$, for some $D \in \mathcal{B}^{r}_{[g(x),0]}(\mathbb{F}_{q^{2^k}})$ or $D \in \mathcal{B}^{r}_{[g^q(x),0]}(\mathbb{F}_{q^{2^k}})$.

ii) Assume that $k \geq 3$ and that there is a nonzero divisor $D_b \in \mathcal{B}^{\infty}_{[x-b,0]}(\mathbb{F}_{q^{2^k}})$ of some level $r \geq 1$. Then every $\bar{D} \in \mathcal{B}^{r}_{[(g(x)),0]}(\mathbb{F}_{q^{2^k}}) \cup \mathcal{B}^{r}_{[(g^q(x)),0]}(\mathbb{F}_{q^{2^k}})$ is of the form $\bar{D} = D + D^{q^2}$ for some $D \in \mathcal{B}^{\infty}_{[x-b,0]}(\mathbb{F}_{q^{2^k}}) \cup \mathcal{B}^{\infty}_{[x-b^q,0]}(\mathbb{F}_{q^{2^k}}) \cup \mathcal{B}^{\infty}_{[x-b^{q^2},0]}(\mathbb{F}_{q^{2^k}}) \cup \mathcal{B}^{\infty}_{[x-b^{q^3},0]}(\mathbb{F}_{q^{2^k}})$.

Proof. The proof is analogous to that of Lemma 6. □

The next propositions show the variation of the exponents of the 2-Sylow subgroup $\mathrm{Jac(C)}[2^\infty](\mathbb{F}_{q^{2^k}})$ when the initial subgroup ($k = 0$) is a cyclic group of order 2 or 4 but not bigger. In our notation this corresponds to

$$r_0 = 1 \text{ and } \nu_0 = 1, 2.$$

From now on, we denote

$$S_k = \text{exponents of } (\mathrm{Jac(C)}(\mathbb{F}_{q^{2^k}})[2^\infty]).$$

Inert types

In the following Proposition we show the values of the 2-Sylow structure for inert types [2,3]. Since $r_0 = 1$, these curves have $f(x) = g(x)h(x)$ over $\mathbb{F}_q[x]$, whose quadratic factor $g(x) = (x - b)(x - b^q)$ over $\mathbb{F}_{q^2}$.

Proposition 4. *The variation of the exponents of $\mathrm{Jac(C)}(\mathbb{F}_{q^{2^k}})[2^\infty]$ for $k = 1, 2$ and inert types [2,3] is shown in Tables 7 and 8.*

S_0	S_1	ν_2	S_2
(1)	(1, 1)	0 (mod 2)	$(n, n), n = \nu_2/2$
(1)	(1, 1)	$2t_1 + 3$	$(n + 1, n), n = (\nu_2 - 1)/2$
(2)	$(\nu_1 - 1, 1)$	$\nu_1 + 2$	$(\nu_1, 2)$

Table 7: Variation of 2-Sylow exponents for inert types, $q \equiv 1 \pmod 4$

Proof. From Table 1 we know that if $r_0 = 1$, then $r_1 = 2$. Since for all cases $\nu_0 = 1$ implies $\nu_1 = 2$ by Tables 3 and 4, clearly $S_0 = (1)$ implies $S_1 = (1, 1)$ in both cases.

S_0	S_1	S_2
(1)	(1,1)	(3,2)
(2)	(2,2)	(3,3)

Table 8: Variation of 2-Sylow exponents inert types, $q \equiv 3 \pmod 4$

Assume $S_0 = (1)$. In order to find the value of S_2 when $q \equiv 1 \pmod 4$, let's consider a divisor $D = [u(x), v(x)]$ in $\mathrm{Jac(C)}(\mathbb{F}_{q^4})$ such that $2^{n-1}D = [x-b, 0]$. By Lemma 6, every divisor $\bar{D}$ such that $2^{n-1}\bar{D} = [g(x), 0]$ is of the form $\bar{D} = D + D^q$ with D in the branch of $[x-b, 0]$ or $[x-b^q, 0]$. Moreover, for our purpose we assume D does not have a bisection (hence clearly D^q has no bisection either). By [4, Thm 4.7], the fact that D has no bisection is equivalent to two of the values in

$$\{u(b), u(b^q), \prod_{i=1}^{3} u(\theta_i)\} \tag{12}$$

not being squares in $\mathbb{F}_{q^4}$. Now, if we take the dereduced representative of $\bar{D}$ (see [4] for more details on this) we have

$$\frac{f(x) - (k(x)\bar{u}(x) + \bar{v}(x))^2}{\bar{u}(x)} = u(x)u^q(x). \tag{13}$$

Assume $u(b)$ is a square in $\mathbb{F}_{q^4}$ and $u(b^q)$ is not. Then, by substitution in (13) it turns out that $\bar{u}(b)$ cannot be a square. Hence, $\bar{D}$ does not have a bisection and thus $S_2 = (n, n)$. The same argument works when $u(b^q)$ is the square in (12). Otherwise, assume the square in (12) is $\prod_{i=1}^{3} u(\theta_i)$. Since neither $u^q(b)$ nor $u^q(b^q)$ are quadratic residues, we deduce $\bar{u}(b)$, $\bar{u}(b^q)$ and $\prod_{i=1}^{3} \bar{u}(\theta_i)$ are squares from (13). Therefore $\bar{D}$ has a bisection over $\mathbb{F}_{q^4}$: there exists $\bar{\bar{D}} = [\bar{\bar{u}}(x), \bar{\bar{v}}(x)] \in \mathrm{Jac(C)}(\mathbb{F}_{q^4})$ such that $2\bar{\bar{D}} = \bar{D} = D + D^q$. Hence,

$$\bar{\bar{u}}(x)^2 = u(x)u^q(x). \tag{14}$$

Since $u(b)$ and $u^q(b)$ are non squares in $\mathbb{F}_{q^4}$, $u(b)u^q(b) = u^{q+1}(b)$ is a square in $\mathbb{F}_{q^4}$. However it cannot be a 4-th power in $\mathbb{F}_{q^4}$ because $q+1 \equiv 2 \pmod 4$. This implies $\bar{\bar{u}}(b)$ can not be a square by (14). Therefore $\bar{\bar{D}}$ has no bisections over $\mathbb{F}_{q^4}$ and D admits one and at most one extra bisection over $\mathbb{F}_{q^4}$. Hence $S_2 = (n+1, n)$.

Assume now $S_0 = (2)$. Over $\mathbb{F}_{q^2}$ the divisor $[g(x), 0]$ of order 2 splits yielding $[x-b, 0], [x-b^q, 0]$. If $q \equiv 1 \pmod 4$ then neither of these have further bisections by *ii)* of Lemma 4, and the value of S_1 follows. If $q \equiv 3 \pmod 4$, then $h(b)h(b^q)$ is a square of $\mathbb{F}_q$ by *i)* of Lemma 4. But this is equivalent to both $h(b), h(b^q)$ being squares of $\mathbb{F}_{q^2}$. Therefore *iii)* of Lemma 4 implies both divisors have a bisection over $\mathbb{F}_{q^2}$. Since $\nu_1 = 4$ from Table 4,

then $S_1 = (2, 2)$. The values of S_2 in this same row in Tables 7 and 8 follow from Proposition 2 and Table 4. □

Split types

In the following Proposition we show the values of the 2-Sylow structure for split types [1,4]. Since $r_0 = 1$, these curves have $f(x) = (x - a)s(x)$ with $s(x) \in \mathbb{F}_q[x]$ irreducible over $\mathbb{F}_q$, with factorization $g(x) = g(x)g^q(x)$ over $\mathbb{F}_{q^2}$ and $s(x) = \prod_{i=0}^{3}(x - b^{q^i})$ over $\mathbb{F}_{q^4}$. We assume $g(x) = (x - b)(x - b^{q^2})$.

Proposition 5. *The variation of the exponents of* $\mathrm{Jac(C)}(\mathbb{F}_{q^{2^k}})[2^\infty]$ *for split types and* $k = 1, 2, 3$ *is shown in Tables 9 and 10.*

S_0	S_2	ν_3	S_3
(1)	(1,1,1,1)	0 (mod 4)	(n, n, n, n), $n = \nu_3/4$
		2 (mod 4)	$(n+1, n+1, n, n)$, $n = (\nu_3 - 2)/4 \geq 2$
		$4t_2 + 7^\dagger$	$(n+1, n+1, n+1, n), n = (\nu_3 - 3)/4 \geq 2$

Table 9: Variation of 2-Sylow exponents for split types, $\nu_0 = 1$.

S_0	S_1	ν_2	S_2
(2)	(2,2)	$8^\dagger$	$(3, 2, 2, 1)$
		0 (mod 2)	$(n, n, 1, 1)$, $n = (\nu_2 - 2)/2 \geq 4$
		1 (mod 2)†	$(n+1, n, 1, 1)$, $n = (\nu_2 - 3)/2 \geq 4$

Table 10: Variation of 2-Sylow exponents for split types, $\nu_0 = 2$.

Proof. For split types, $r_0 = 1$ implies $r_1 = 2$ and $r_2 = 4$ by Table 1. Regarding Table 9, $\nu_0 = 1$ implies $\nu_1 = 2$ and $\nu_2 = 4$ by Tables 5 and 6. Hence $S_0 = (1)$ implies $S_1 = (1, 1)$ and $S_2 = (1, 1, 1, 1)$. Consider now a divisor $D = [u(x), v(x)]$ in $\mathbb{F}_{q^8}$ with no bisection and such that $2^{n-1}D = [x - b, 0]$. By [4, Thm 4.7], this is equivalent to a nonzero even number of the values in $\{u(a), u(b), u(b^q), u(b^{q^2}), u(b^{q^3})\}$ not being squares in $\mathbb{F}_{q^8}$. Clearly, the conjugates $D^{q^i} = [u^{q^i}(x), v^{q^i}(x)]$ do not have further bisections either and they satisfy

$$\begin{aligned}
2^{n-1}D^{q^i} &= [x - b^{q^i}, 0], \\
2^{n-1}(D^{q^i} + D^{q^j}) &= [(x - b^{q^i})(x - b^{q^j}), 0], \quad i, j = 0, \ldots, 3, i \neq j, \\
2^{n-1}(D + D^q + D^{q^2} + D^{q^3}) &= [x - a, 0], \\
2^{n-1}(D + D^q + D^{q^2}) &= [(x - a)(x - b^{q^3}), 0],
\end{aligned}$$

†Only when $a_0 \neq 0$.

and so on. We have to find out if some sum of the conjugates D, D^q, D^{q^2}, D^{q^3} has a further bisection.

- Assume $u(a)$ is a non-square in $\mathbb{F}_{q^8}$. Then there are 1 or 3 non-squares in $\{u(b), u(b^q), u(b^{q^2}), u(b^{q^3})\}$. By *ii)* of Lemma 7, every divisor $\bar{D}$ such that $2^{n-1}\bar{D} = [g(x), 0]$ is of the form $\bar{D} = D + D^{q^2}$ with D in some branch $[x - b^{q^i}, 0]$. We can find an appropriate b^{q^j} such that the evaluation of the first coordinate of $\bar{D}$ at b^{q^j} is a non square of $\mathbb{F}_{q^8}$. For example assume there is just 1 non-square and that it is $u(b)$. Then $u^{q^2}(b) = (u(b^{q^2}))^{q^2}$ is the conjugate of a square, hence a square. Now, from the dereduced identity

$$\frac{f(x) - (k(x)\bar{u}(x) + \bar{v}(x))^2}{\bar{u}(x)} = u(x)u^{q^2}(x) \tag{15}$$

  we deduce $\bar{u}(b)$ and $\bar{u}(b^{q^2})$ are the non squares. Hence $\bar{D}$ does not have a bisection. The same argument works for the branch of $[g^q(x), 0]$. Consider now a divisor D' such that $2^{n-1}D' = [(x - a), 0]$. By *i)* of Lemma 7, $D' = \bar{D} + \bar{D}^q$, with $\bar{D}$ in the branch of $[g(x), 0]$ or $[g^q(x), 0]$. Assuming, as above, that $\bar{u}(b^q)$ is a square and $\bar{u}(b)$ is not, we derive $u'(b)$ is not a square from the dereduced identity (13). Therefore, D' does not have a bisection. The previous cases rule out the possible bisections of $\bar{D}$ in the remaining branches of $[(x - b^{q^i})(x - b^{q^{i+1}}), 0]$ or $[(x - a)(x - b^{q^i}), 0]$ by contradiction. Hence $S_3 = (n, n, n, n)$.

- Assume $u(a)$ is a square in $\mathbb{F}_{q^8}$. Then there are 2 or 4 non-squares in $\{u(b), u(b^q), u(b^{q^2}), u(b^{q^3})\}$. Assume first there are just 2 non-squares. Since conjugation (by q and also by q^2) respects both squares and non-squares, we can assume the non-squares are $u(b), u(b^{q^2})$. Then, every divisor $\bar{D} = D + D^{q^2}$ such that $2^{n-1}\bar{D} = [g(x), 0]$ has a bisection by evaluating (15) at any conjugate of b. Similarly, every $D' = \bar{D} + \bar{D}^q$ has a bisection which has no successive bisections by *ii)* of Lemma 7. Hence $S_3 = (n + 1, n + 1, n, n)$.

  Finally, assume none of $u(b^{q^i})$ is a square. Then the sums $\bar{D}$ of 2 conjugates of D do have a bisection $\bar{\bar{D}}$. Again by *ii)* of Lemma 7 no $\bar{\bar{D}}$ has a further bisection. Besides, every $D' = \bar{D} + \bar{D}^q$ such that $2^{n-1}\bar{D} = [x - a, 0]$ has a bisection, but does not have a further bisection. Hence $S_3 = (n + 1, n + 1, n + 1, n)$.

Regarding S_1 in Table 10, since $s(a)$ is a square in $\mathbb{F}_q$ if and only if $g(a)$ and $g(a)^q$ are squares in $\mathbb{F}_{q^2}$, then $[g(x), 0]$ and $[g^q(x), 0]$ do have bisections by *i)* and *ii)* of Lemma 5. Therefore $S_1 = (2, 2)$. About S_2, since $q^2 \equiv 1 \pmod 4$, then $b - b^{q^2}$ is not a square in $\mathbb{F}_{q^4}$ (and neither is the conjugate $b^q - b^{q^3}$). Therefore the divisors $[x - b^{q^i}, 0]$ do not have bisections in $\mathbb{F}_{q^4}$ for

$i = 0, \ldots, 3$ by *iii*) of Lemma 5. The remaining differences $b - b^q, b - b^{q^3} = (b^q - b)^{q^3}, b^{q^2} - b^{q^3} = (b - b^q)^{q^2}$ being non-squares (hence only $b - b^q$ is a non-square) determines the case $(3, 2, 2, 1)$ since then all sums of (2 to 4) conjugates of $[x - b, 0]$ do have a bisection indeed. Otherwise, the exponents of S_2 have the form $(n', n, 1, 1)$. Let $D = [u(x), v(x)]$ in $\mathbb{F}_{q^4}$ with no bisection and such that $2^{n-1}D = [g(x), 0]$. Then $u(a)$ being a square or not determines the cases $(n + 1, n, 1, 1)$ and $(n, n, 1, 1)$ respectively by *i*) of Lemma 7. □

References

[1] P. Gaudry, É. Schost. *Genus* 2 *point counting over prime fields*, Journal of Symbolic Computation 47 (2012), no. 4, 368–400.

[2] D. Maisner, E. Nart. *Abelian surfaces over finite fields as Jacobians*, Experimental Mathematics 11 (2002), 321-327.

[3] J. Miret, J. Pujolàs, A. Rio. *Bisection for genus 2 curves in odd characteristic*, Proceedings of the Japan Academy Series A Mathematical Sciences 85 (2009), no. 4, 55-60.

[4] J. Miret, J. Pujolàs, N. Thériault. *Bisection and squares in genus 2*, Finite Fields and Their Applications 36 (2015), 170-188.

[5] J. Miret, J. Pujolàs, N. Thériault. *Bisection for genus 2 curves with a real model*, Bulletin of the Belgian Mathematical Society 22 (2015), no. 4, 589-602.

[6] H.-G. Rück. *Abelian surfaces and Jacobian varieties over finite fields*, Compositio Mathematica 76 (1990), no. 3, 351-366.

[7] R. Schoof. *Nonsingular plane cubic curves over finite fields*, Journal of Combinatorial Theory. Series A 46 (1987), no. 2, 183-208.

[8] L. C. Washington. Introduction to cyclotomic fields. Second edition. Graduate Texts in Mathematics, 83. Springer-Verlag, New York, 1997.